REMARKS

Claims 1-3, 5, 7-13, 18-24, and 28-31 are currently pending in this application. Claims 1-3, 5, 7-13, 18-24, and 28-31 have been rejected. The response amends claims 1, 2, 18, 23, 28 and 29. Reconsideration and withdrawal of the rejections set forth in the Office Action dated June 1, 2007, are respectfully requested.

Claim Rejections

Claims 1-3, 5, 8-13, 18-24 and 28-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis et al. (U.S. Patent 6,233,565 B1) herein referred to as Lewis in view of Korn et al. (U.S. Patent 6,442,607 B1) herein referred to as Korn.

The Prior Art

Lewis apparently discloses:

> A system and methods for conducting Internet based financial transactions between a client and a server... A transaction module is included wherein, in response to the client and server being authenticated, the client issues a transaction request to the server and the transaction server, in response to a client transaction request, executes an electronic payment transaction at the server and records the transaction in the transaction database... In addition, a third party seller having a processor and a database can be connected via a communication channel to the server, wherein the client further obtains a registration certificate representative of being a consumer registered with said third party seller. A third party credit facility also may be connected via a communication link to the server, for implementing credit card transactions. The transaction execution system may be to purchase an amount of postage, to purchase a ticket for air travel or to an entertainment complex or the like. (Abstract).

The applicants respectfully point out that the Examiner has missed the significance of arguments presented in the paper responsive to the Office Action dated January 9, 2007. Specifically, Lewis does not teach encrypting data at a point between the client and the server. In the Examiner's Response to Arguments on pages 3-4 of the present Office Action, the Examiner did not address this issue. As is described below and apparent from the amendments to the claims, the applicants have attempted to clarify that an apparatus is positioned between the client and the server. Lewis does not disclose this.

Korn apparently discloses

> A method includes receiving a stream of data in a computer for transmission from the computer. A determination is made whether a portion of the stream of data indicates personal information. Based on the determination, action is automatically taken to control transmission of the portion of the stream. The method may be performed, for example, by a processor of the computer. (Abstract).

The data identification and blocking in Korn happens as the content is typed in by the client at a keyboard before the data even reaches the operating system of the client computer (col. 3, lines 8-10). There is no apparatus positioned between the computer and a server.

Neither Lewis nor Korn teach checking the received content before it reaches components in a server environment, which is important for protecting sensitive user data in the content from being exposed to unauthorized access ***after*** the content has been sent from the client. Moreover, neither Lewis nor Korn disclose encrypting data at a point between the client and the server. This is significant because the client may not be aware of what should be encrypted, may not be able to encrypt in a manner that is usable by the system, may not be the best place for making encryption decisions, or may not be the best choice for other reasons; while the server environment may not be completely secure or may have no business knowing certain data.

The Prior Art Distinguished

To render a claim obvious, the prior art, whether considered alone or in combination, must teach each and every element of the claim. Independent claim 1 includes the language:

> a server having a server environment, wherein, in a first stage, the server and a client are coupled using a protocol to establish at least one secure channel;
>
> an appliance, wherein in a second stage the appliance is inserted between the client and the server, wherein the protocol is pre-existing because it was used in the first stage to couple the client and the server…

Neither Lewis nor Korn disclose an appliance that is inserted between a client and a server using a pre-existing protocol. It should be noted that, in claim 1, the client and server have a secure channel, and the appliance is nevertheless inserted between them. For at least these reasons, claim 1 is allowable over the cited prior art, whether considered alone or in combination.

Claim 1 further includes the language that the appliance:

> intercepts at least one electronic transaction query from the at least one client via at least one secure channel using the pre-existing protocol;
>
> evaluates the at least one electronic transaction query for sensitive data;
>
> encrypts the specified sensitive data;
>
> transfers, using the pre-existing protocol, the encrypted sensitive data among components of the server environment, wherein the server is substantially incapable of distinguishing between data from the client that does not pass through the appliance and data from the client that was

intercepted by the appliance, and wherein the encrypted sensitive data is stored in one or more components of the server environment;

receives at least one electronic information query for the encrypted sensitive data from at least one third-party system via the at least one secure channel;

obtains the encrypted sensitive data from the server;

decrypts the encrypted sensitive data in response to the at least one electronic information query;

provides the decrypted sensitive data to the at least one third-party system via at least one secure coupling.

Neither Lewis nor Korn disclose an apparatus that intercepts transmissions between client and server. Intercept, as is well understood, includes a meaning that the electronic transaction query was sent (from the perspective of the client) to the server. That is, the client did not explicitly send the electronic transaction query to the apparatus. Then, ***outside of both the client and server environments***, the apparatus evaluates the query for sensitive data. Lewis and Korn do not disclose this.

Even though the appliance intercepted a query from the client to the server, where the client and the server are coupled via the pre-existing protocol, the appliance nevertheless transmits the encrypted sensitive data ***using the pre-existing protocol***. Lewis and Korn do not disclose this.

The server is substantially incapable of distinguishing between data as sent from the client and data as encrypted at the appliance. Thus, ***neither the client nor the server necessarily know how to decrypt the sensitive data***. Such a teaching is found in neither Lewis nor Korn. When a third party requests the sensitive data, it is up to the appliance to obtain and decrypt the sensitive data for the third party; the server cannot provide it directly. For at least these additional reasons, claim 1 is allowable over the cited prior art, whether considered alone or in combination.

Claim 2 includes the language:

> evaluating at least one electronic request received from a client over at least one secure channel established, using a communication protocol, between the client and a server having an associated server environment;
>
> applying at least one cryptographic operation to sensitive data specified in response to the at least one electronic request, yielding sensitive data in a first form;
>
> transmitting the sensitive data in the first form to the server using the communication protocol, wherein the sensitive data in the first form is encrypted, yielding sensitive data in a second form, before transfer among components of the server environment, wherein the sensitive data in the second form is decrypted, yielding the sensitive data in the first form, before transfer from the server environment.

Although claim 2 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. For example, a client and server have established a secure channel using a communication protocol, but a device other than the server nevertheless receives an electronic request from the client over the secure channel.

Claim 2 further includes the language "transmitting the sensitive data in the first form to the server using the communication protocol, wherein the sensitive data in the first form is encrypted, yielding sensitive data in a second form, before transfer among components of the server environment, wherein the sensitive data in the second form is decrypted, yielding the sensitive data in the first form, before transfer from the server environment." This language indicates a component of the server encrypts the data (perhaps again). Neither Lewis nor Korn disclose "double-encryption" or a comparable operation. Accordingly, claim 2 is allowable over the cited prior art, whether considered alone or in combination, for at least this additional reason. Claims 3, 5, 7-13, which depend from claim 2, are allowable at least for depending from an allowable base claim and potentially for other reasons, as well.

Claim 18 includes the language:

> at least one client computer coupled to at least one server site using a network protocol to establish at least one secure channel over at least one network;
>
> at least one processing device coupled among the at least one server site, the at least one client computer and the at least one network, wherein, in operation, the at least one processing device evaluates at least one electronic request from the at least one client computer to the at least one server site received via the at least one network and applies at least one cryptographic operation to the sensitive data in response to the at least one electronic request,
>
> wherein the sensitive data of the at least one electronic request is encrypted prior to transfer among components of the at least one server site,
>
> wherein encrypted sensitive data of the at least one server site is decrypted prior to transfer among the at least one network.

Although claim 18 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. For example, a client computer is coupled to a server site using a network protocol to establish a secure channel. The processing device is coupled among the various components and evaluates an (intercepted) electronic request sent from the client computer to the server site. Claims 19-22, which depend from claim 18, are allowable at least for depending from an allowable base claim, and potentially for other reasons as well.

Claim 23 includes the language:

at least one processing device coupled among at least one server system and at least one network coupling to evaluate at least one received electronic request in a first protocol format, wherein the at least one processing device:

determines whether the at least one received electronic request includes sensitive data;

encrypts the sensitive data;

reforms the electronic request, including the encrypted sensitive data, without deviating from the parameters of the first protocol format,

transfers the reformed electronic request, in the first protocol format, to at least one component of the at least one server system.

Although claim 23 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. For example, the processing device is coupled among components of a server system and a network, and receives an electronic request in a first protocol format, and transfers the electronic request in the first protocol format after reforming it.

In addition, claim 23 includes language that the electronic request is reformed without deviating from the first protocol format. Lewis and Korn do not disclose this. Accordingly, claim 23 is allowable over the cited prior art, whether considered alone or in combination, for at least this additional reason. Claim 24, which depends from claim 23, is allowable at least for depending from an allowable base claim, and potentially for other reasons as well.

Claim 28 includes the language:

means for receiving at least one electronic transaction query from at least one client computer via at least one secure coupling using a protocol agreed upon by the at least one client computer and at least one server having an associated server environment;

means for evaluating the at least one electronic transaction query for sensitive data;

means for encrypting the specified sensitive data;

means for transparently transferring, using the protocol agreed upon by the at least one client computer and the at least one server, the encrypted sensitive data among components of the server environment;

means for receiving at least one electronic information query for the encrypted sensitive data from at least one third-party system via the at least one secure coupling;

means for decrypting the encrypted sensitive data in response to the at least one electronic information query; and

means for transferring the decrypted sensitive data to the at least one third-party system via the at least one secure coupling.

Although claim 28 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. For example, an electronic transaction query is received from a client computer via a secure coupling using a protocol agreed upon by the client computer and a server.

In addition, claim 28 includes language that the electronic request is transparently transferred to the server using the protocol agreed upon by the client computer. Lewis and Korn do not disclose transparently transferring data from the client to the server. Accordingly, claim 28 is allowable over the cited prior art, whether considered alone or in combination, for at least this additional reason.

Claim 29 includes the language:

a processor;

a network interface coupled to the processor;

a pattern specification engine coupled to the processor,

a cryptographic engine coupled to the processor;

wherein, in operation,

a client and server establish a connection in accordance with a first protocol;

first one or more packets sent from the client to the server including payload formatted in a first protocol are input on the network interface;

the pattern specification engine enables a user to apply a regular expression to the payload to specify which portion of the payload includes sensitive data to be encrypted and which portion of the payload includes non-sensitive data before the payload reaches the server;

the cryptographic engine applies a cryptographic transformation to the sensitive data;

the processor forms second one or more packets, having the client as source and the server as destination, including the cryptographically transformed sensitive data and the non-sensitive data in the first protocol;

the second one or more packets are output on the network interface.

Although claim 29 has different language than claim 1, which is intended to ensure broad coverage of inventive aspects and potentially differing scopes, the same principles as described with reference to claim 1 apply. For example, a client and server establish a connection in accordance with a first protocol, and packets from the client are input to a network interface and data is cryptographically transformed prior to being sent along to the server in the first protocol. Claims 30-31, which depend from claim 29 are allowable at least for depending from an allowable base claim.

Conclusion

In light of the amendments and the preceding arguments, the applicant respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance.

If the Examiner believes that a conference would be of value in expediting the prosecution of this application, he is cordially invited to telephone the undersigned counsel at (650) 838-4305 to arrange for such a conference.

No fees are believed to be due; however, the Commissioner is authorized to charge any underpayment in fees to Deposit Account No. 50-2207.

Respectfully submitted,

Date: September 4, 2007

/William F. Ahmann/
William F. Ahmann
Reg. No. 52,548

Correspondence Address:
Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, CA 94026-2168
(650) 838-4300